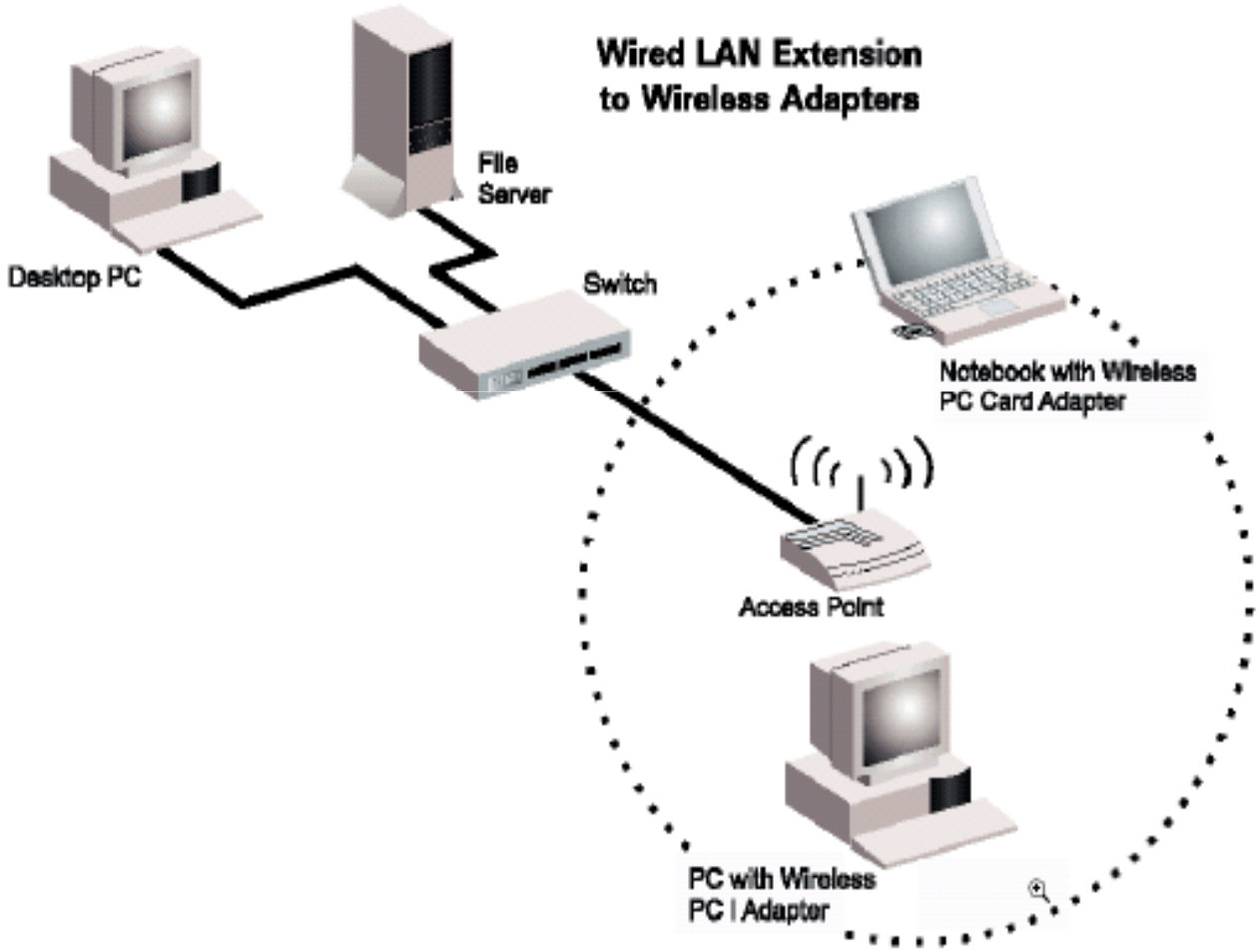
Wireless Hacking

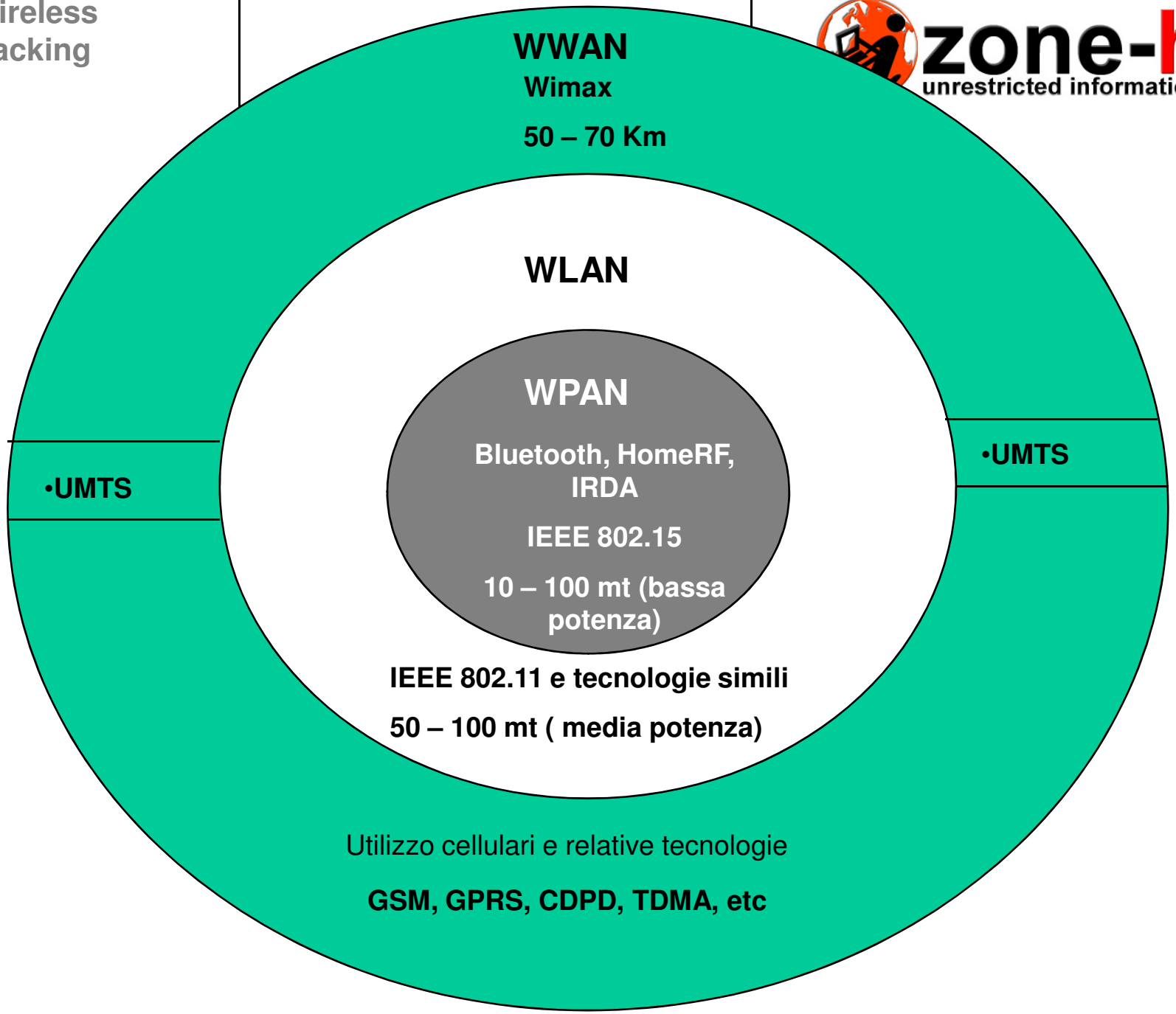


Docente

•Luigi D'Amato, Senior CyberSecurity Consultant e CTO di Security Lab SAGL, Luigi è docente di lungo corso dei corsi Zone-h in Italia e Svizzera, ma è anche stato l'artefice dell'introduzione del corso Wireless Hacking in Paesi quali il Giappone, Estonia, e Norvegia.
Certificato CWNA, Cisco CCNA e WLAN FE.
Membro ufficiale del chapter italiano dell' Honeynet Project Alliance Research.
Specializzato in Botnet Analysis, Malware Analysis
Monitoring, Tracking, Intelligence, Penetration testing, Vulnerability assesment.

•Mail: luigi.damato@sec-lab.com

•Skype: secwireless



Lo standard 802.11 delle Wireless LAN

Standard IEEE per le Wireless LAN Wireless

-1990: Viene creato il gruppo di studio

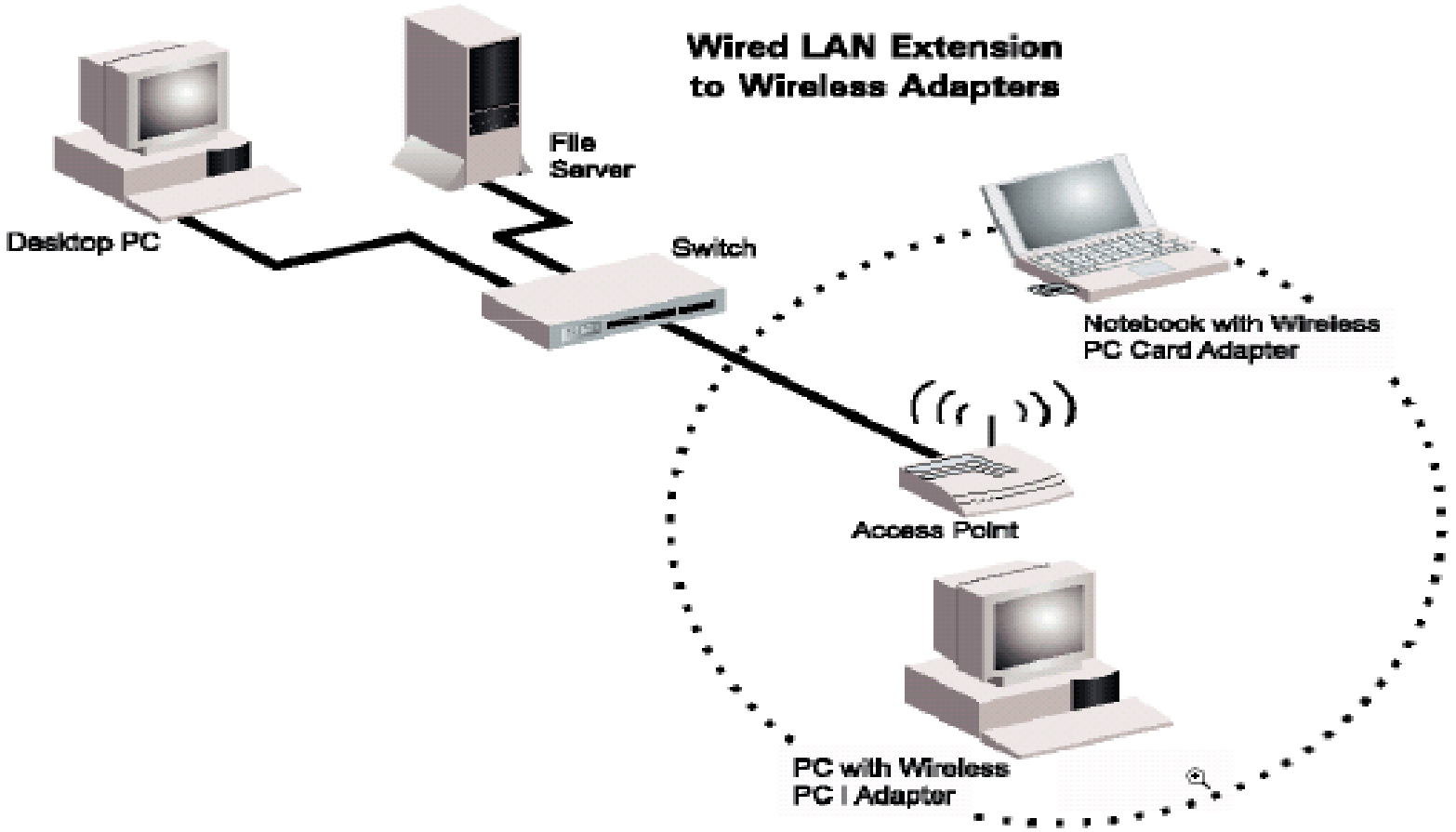
-1997: Approvato lo standard base 802.11-key a 40 bit

-1999: Creata la versione ad “alta” velocità ed incrementata la “sicurezza” – key a 104 bit

Creati i task group per le evoluzioni dello standard “a – i”

Modalità ad-hoc

Modalità Infrastructure



Estensioni successive

-**802.11b** è l'estensione del PHY 802.11 nella banda a 2.4 GHz per il supporto di 5.5 e 11 Mbit/sec, in tecnologia DSSS

- Esistono implementazioni proprietarie non standard che portano la velocità a 22 Mbit/s

-**802.11g/a** è l'estensione del PHY 802.11 nella banda a 2.4 GHz (802.11g) o 5 Ghz (802.11a), supporta fino a 54 Mbit/sec, in tecnologia Orthogonal Frequency Division Multiplex (OFDM), l'802.11g è compatibile con 802.11b

- Esistono implementazioni proprietarie non standard che portano la velocità >100 Mbps

-**802.11n** nuovo standard che permetterà di aumentare la velocità fino a 540 Mbps e/o di aumentare il raggio di copertura. Usando la tecnologia MIMO (Multiple Input Multiple Output)

- Esistono dispositivi pre-standard che usano la tecnologia MIMO. Attenzione: non è detto che questi device saranno aggiornabili all'802.11n definitivo

Lo strato FISICO 802.11

Lo scopo del livello fisico è:

fornire un canale per la comunicazione attraverso l'utilizzo di specifiche riguardanti la parte elettrica, meccanica e procedurale

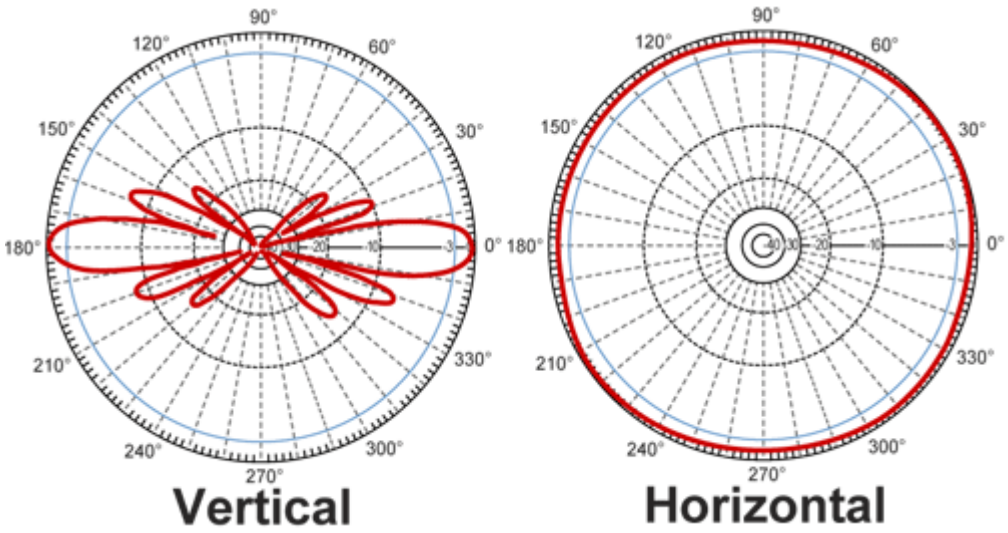
<table>
<tr><td colspan="3">802.2</td><td rowspan="2">Data Link Layer</td></tr>
<tr><td colspan="3">802.11 MAC</td></tr>
<tr><td>FH</td><td>DS</td><td>IR</td><td>PHY Layer</td></tr>
</table>

Antenne

Possiamo utilizzare diversi tipi di antenne a seconda della necessità:

- Omnidirezionali (il segnale viene irrorato e ricevuto a 360°) molto utile per cercare reti senza una direzione prefissata

  Ottime per coprire aree più estese

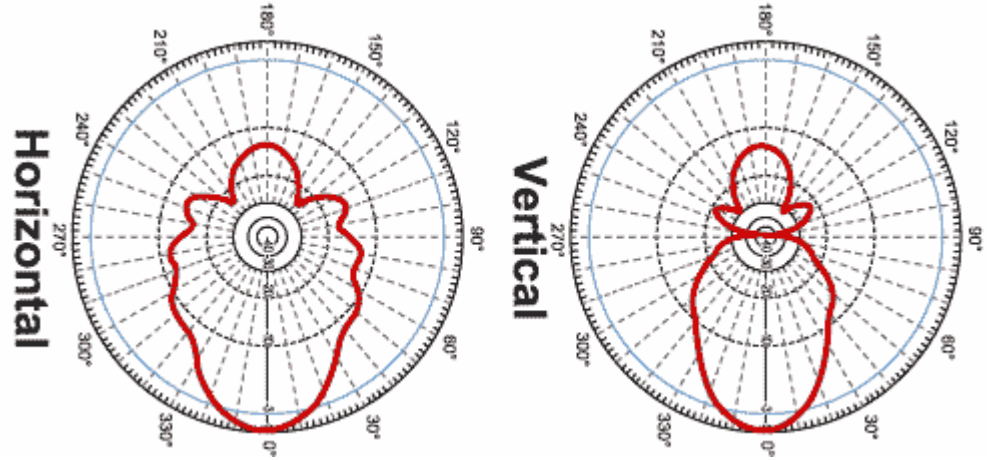


Antenne 2

•Direzionali e Semi-direzionali:

Irrorano e ricevono il segnale secondo delle direzioni ben precise o secondo determinate angolazioni

Ottime per collegamenti a lunga distanza



Come funzionano gli scanner wireless? (2)

•Scansione di tipo PASSIVA

• La maggior parte degli AP possono essere settati in modo da evitare che lo SSID venga mandato in un FRAME PROBE RESPONSE, o evitare di spedire in broadcast il FRAME di BEACON

•Analizzando il protocollo si evince che lo SSID viene comunicato anche in:

- •Associazione
- •Riassociazione
- •Beacon

•Scanner di tipo passivo:

- •Kismet, Airtraf

Metodi di protezione offerti dallo standard

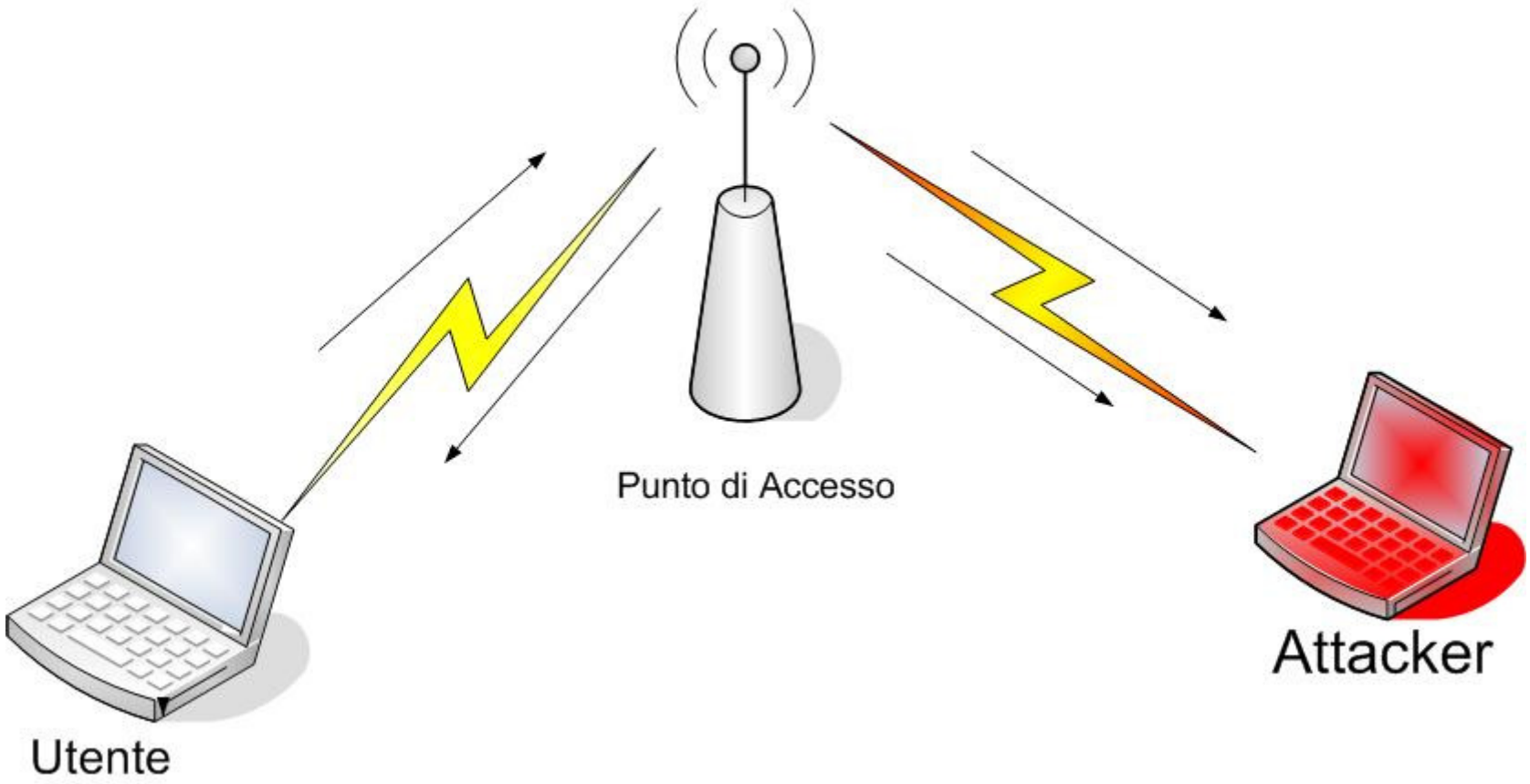
- Lo standard 802.11 stabilisce le seguenti protezioni:
  - SSID hide
  - L'utilizzo del MAC FILTERING (si possono abilitare sull'Access Point i client che sono abilitati ad essere associati allo stesso)
  - L'utilizzo dell'algoritmo WEP
  - WPA (in modalità HOME (PSK) o in modalità Enterprise

Attacchi contro le Wireless LAN

- ✓ Eavesdropping;
- ✓ Jamming;
- ✓ Attacchi injection e di modifica dei dati;
- ✓ Client e punti di accesso (AP) alla rete fraudolenti;
- ✓ Pericoli legati alla crittografia.

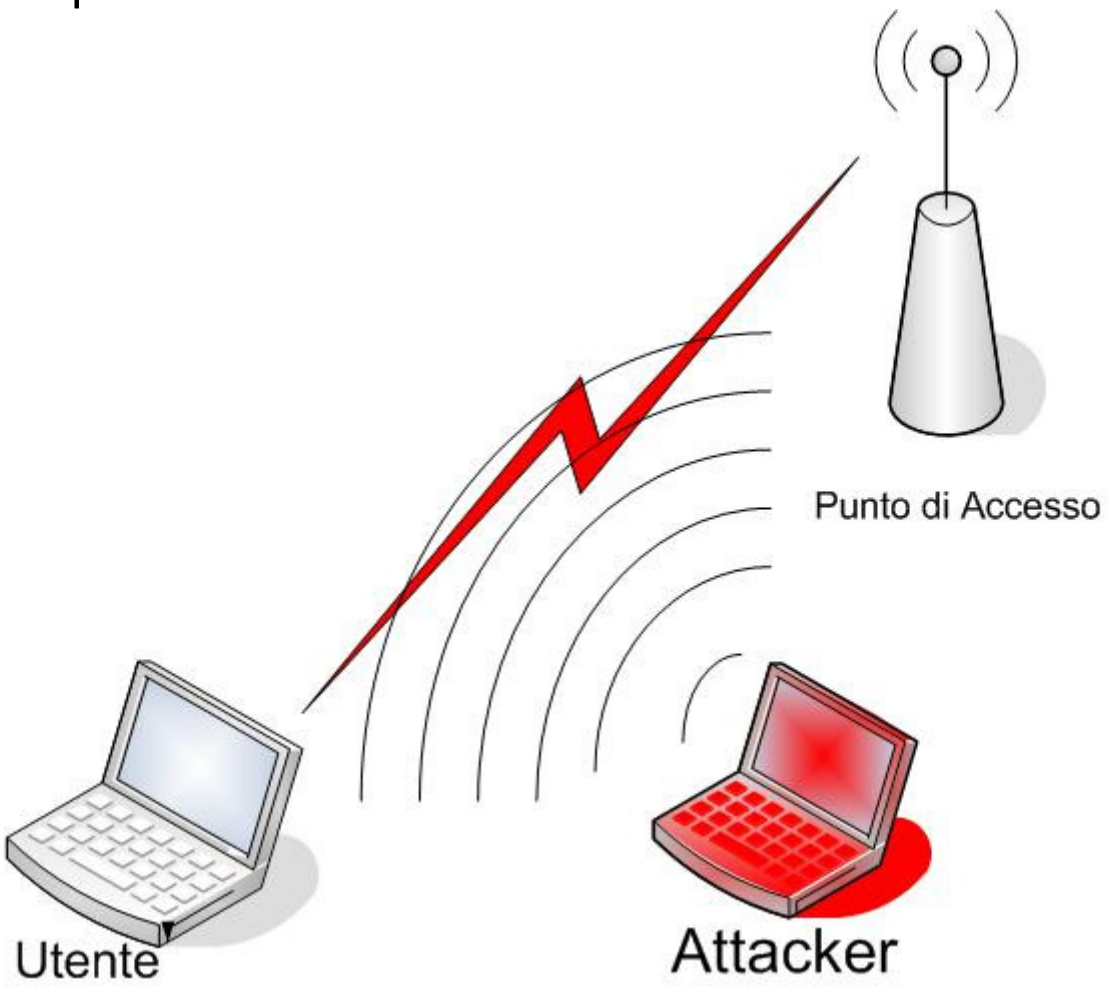
Eavesdropping

Attraverso questo attacco un malintenzionato potrebbe intercettare e decodificare i segnali radio, utilizzando apparecchiature semplici quanto quelle usate per accedere alla lan stessa.



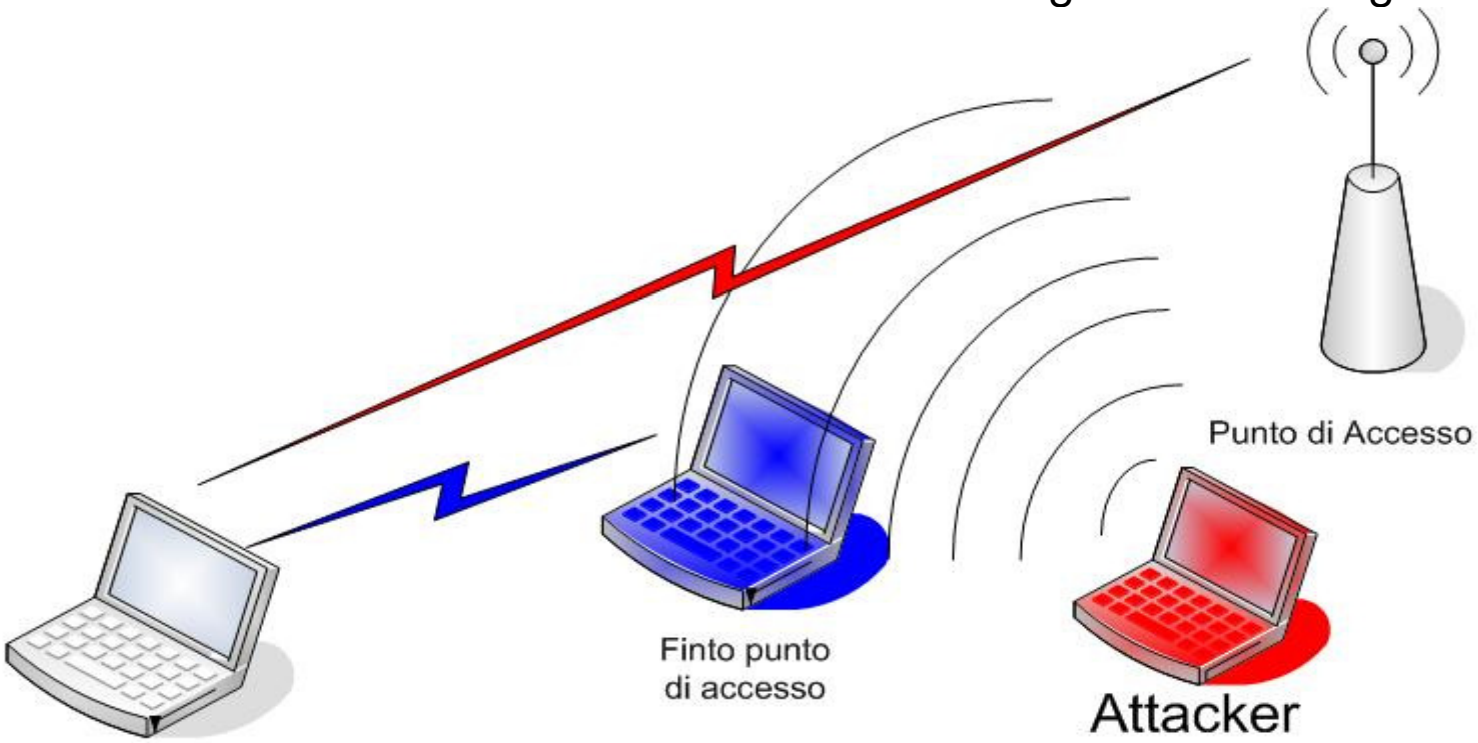
Jamming 1

L'attacco "*Jamming*" invece si verifica quando si provoca accidentalmente o intenzionalmente delle interferenze, rendendo praticamente inutilizzabile il canale di comunicazione.



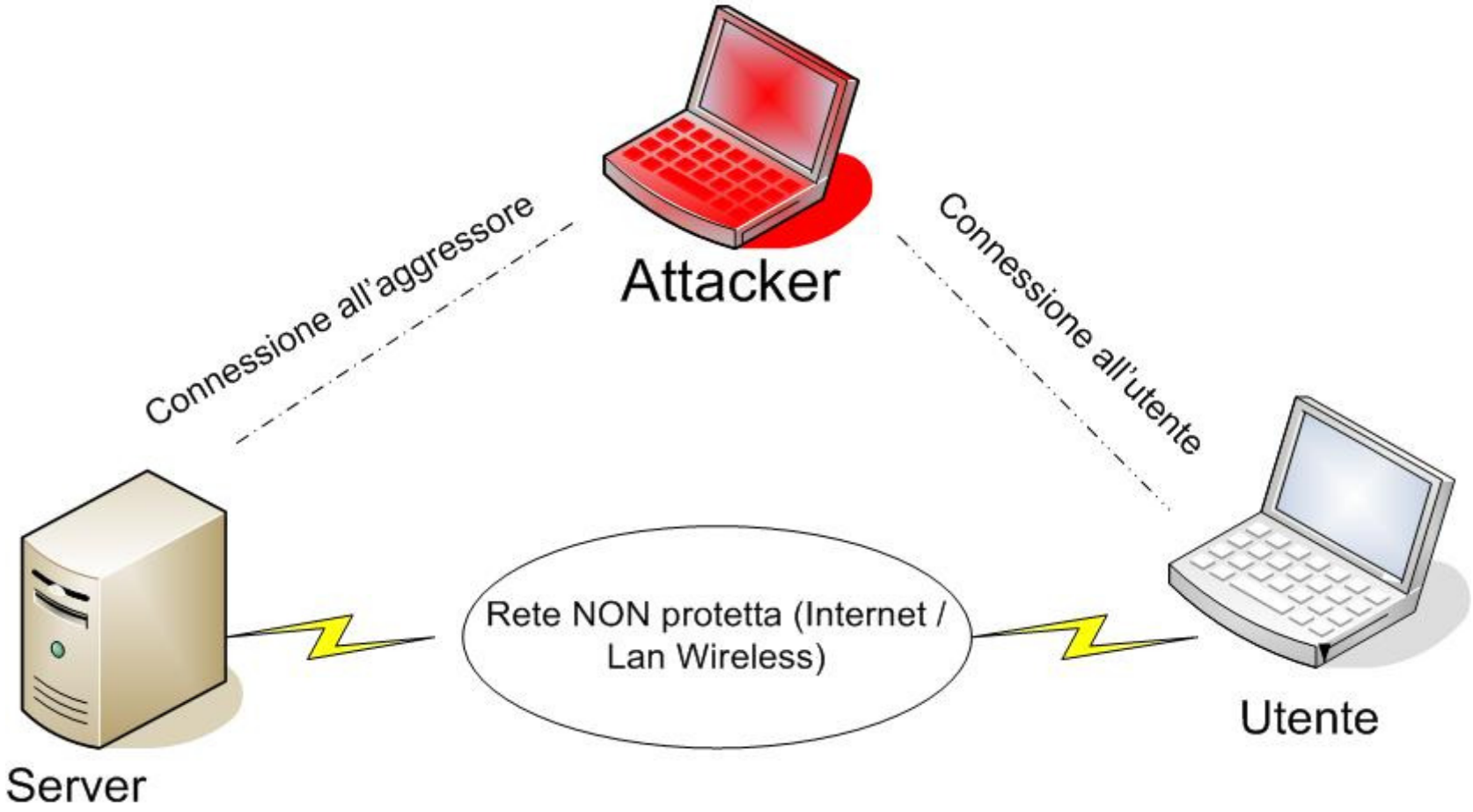
Jamming 2

Un aggressore potrebbe protrarre questo attacco verso il punto di Accesso e oltre all'interruzione delle comunicazioni tra il client ed il punto di accesso, fare in modo di dirottare le comunicazioni verso un'altra stazione facendola figurare come legittima.



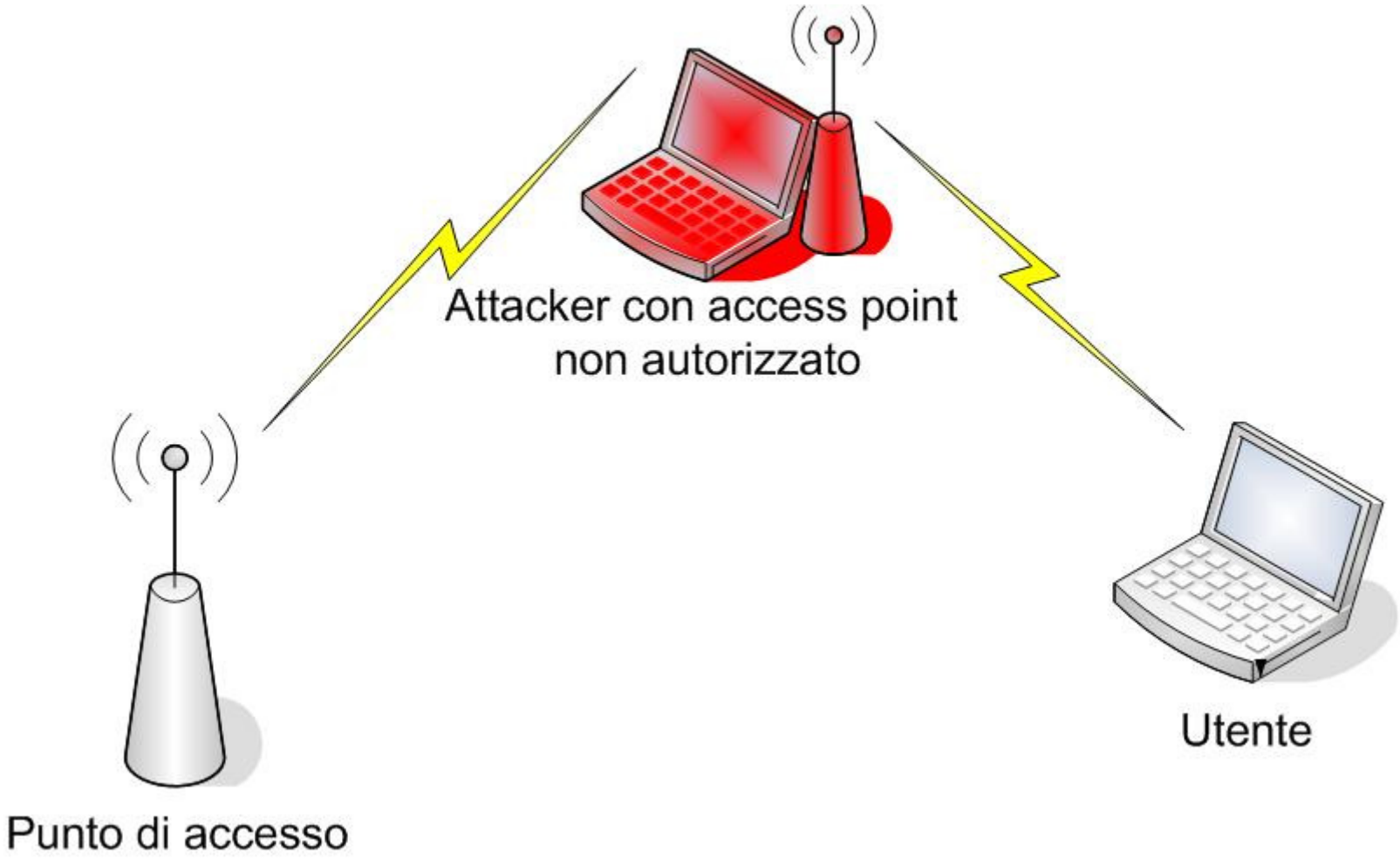
Attacco Inject e modifica di dati

Un attacco injection si verifica quando un aggressore aggiunge dati a una connessione esistente per dirottarla o per inviare senza permesso dei comandi.



Client e Access Point fraudolenti

Un aggressore può definire un punto di accesso fraudolento, in modo da poter accedere alle risorse di rete

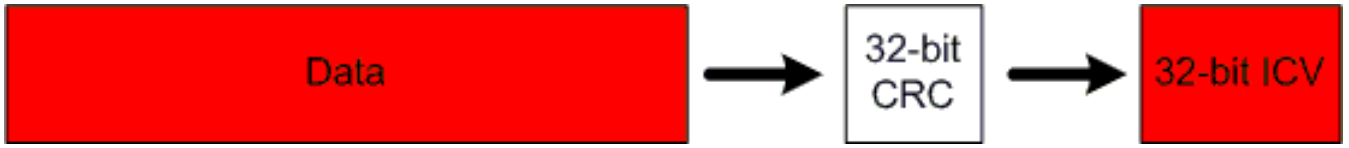


Funzionamento del WEP

Come crittografa i DATI

Messaggio in chiaro “M”

1

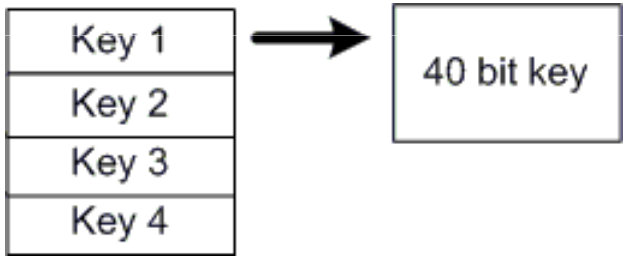


Primo passaggio :
Viene calcolato un checksum del messaggio M, che consente di verificare successivamente l’integrità del messaggio.

***Nota**: Il checksum CRC32 è una funzione unkeyed (senza chiavi) lineare; di conseguenza il pacchetto può essere modificato in modo da ottenere lo stesso checksum (BIT FLIPPING)*

2. 

Viene creato un flusso di byte di lunghezza
24 bit denominato “IV” (Vettore di inizializzazione)

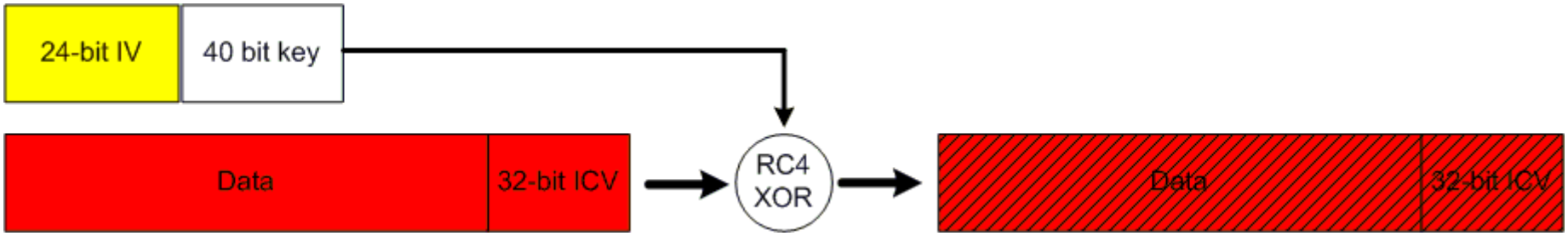
3. 

Viene scelta una delle chiavi “inserite precedentemente”

4. 

Il vettore di inizializzazione viene aggiunto alla key, “SEME”

Come crittografa i DATI 3



5. Il valore del “Seme” viene trasferito a RC4 che genera un keystream.

6. Viene applicato l’operatore XOR al keystream e viene prodotto il testo cifrato.

Come crittografa i DATI 4

7. Vengono aggiunti gli HEADER 802.11 e il vettore di inizializzazione “IV”.

PLAINTEXT(Testo in chiaro):

1	1	0	1	0	0	1	1

XOR

KEYSTREAM (Chiave WEP + IV):

1	0	1	0	0	1	1	0

Cipher text (Testo cifrato): =

0	1	1	1	0	1	0	1

XOR

KEYSTREAM (Chiave WEP + IV):

1	0	1	0	0	1	1	0

=

PLAINTEXT (Testo in chiaro):

1	1	0	1	0	0	1	1

WPA add-on al WEP

- Nuovo algoritmo che sostituisse il Wep fu considerato IMPROPONIBILE
- Parte del nuovo standard 802.11i
- Richiede solo un upgrade del firmware
- Corregge i problemi del WEP, vediamo come:

Patch: Integrity Check Value (ICV)

- WEP utilizza una funzione lineare CRC 32 (vulnerabile al bit flipping)
- WPA utilizza una funzione “MIC” o Michael è una funzione one-way creata da “Neils Ferguson”
- Scoperte due vulnerabilità: Brute Forcing e D.o.S

Patch: Forgery and Replay

WPA - vettore di inizializzazione a 48 bit, creato in maniera particolare:

1) MAC address sending card + sequential counter value

2) Controllo sul sequential counter

Patch: User Authentication

WEP: offre shared authentication system, ma come abbiamo visto è inservibile!

WPA: 802.1x Extensible Authentication Protocol over LAN (EAPoL), di solito con un RADIUS server.

WPA – PSK viene utilizzata una chiave condivisa.

PACCHETTO WEP

PACCHETTO WPA